That which is claimed is:

1. A method of providing secure communications between a first and a second communications unit, the method comprising a key exchange between the first and second communications units resulting in a shared secret key, the key exchange including a user interaction, the method comprising the steps of:

providing, at least partly by means of a user interaction, a passcode to the first and second communications units;

generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit, and transmitting each generated contribution to the corresponding other communications unit;

authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on at least the passcode; and

establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully.

2. A method according to claim 1, wherein the passcode is short enough to be communicated via a user interaction.

3. A method according to claim 1, further comprising:

encrypting the passcode by the second communications unit using the generated shared secret key;

transmitting the encrypted passcode to the first communications unit together with the generated second contribution;

decrypting the received encrypted passcode by the first communications unit; and

comparing the decrypted received passcode with the passcode provided to the first communications unit to authenticate the received second contribution.

4. A method according to claim 1, wherein the first and second contributions are first and second public keys of a Diffie-Hellman key exchange protocol.

5. A method according to claim 1, wherein the step of providing a passcode to the first and second communications units comprises generating a passcode by the first communications unit and providing the generated passcode to the second communications unit via a communications channel including a user interaction.

6. A method according to claim 1, wherein the step of authenticating the transmitted first and second contributions comprises authenticating the first contribution by calculating a tag value of a message authentication code, the tag value being calculated from the first contribution and the passcode.

7. A method according to claim 6, wherein the tag value is calculated by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode.

8. A method according to claim 7, further comprising calculating a hash value of a one-way hash function from the first contribution and calculating said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode.

9. A method according to claim 7, wherein the error correcting code is a Reed-Solomon code.

10. A method according to claim 1, comprising:

generating the first contribution to the shared secret key by the first communications unit, and transmitting the generated first contribution to the second communications unit;

authenticating the received first contribution by the second communications unit based on the passcode, and generating the shared secret key from at least the received first contribution, if the received first contribution is accepted as authentic;

transmitting a second contribution to the shared secret key generated by the second communications unit to the first communications unit; and

authenticating the received second contribution by the first communications unit based on the passcode; and generating the shared secret key by the second communications unit only if the received first contribution is accepted as authentic.

11. A method according to claim 10, wherein the method further comprises:

calculating a first message tag of a message authentication code from the first contribution using the passcode as a key; and

providing the calculated first message tag to the second communications unit; and

wherein the step of authenticating the received first contribution by the second communications unit based on the passcode comprises:

calculating a second message tag of said message authentication code from the received first contribution using the passcode as a key; and

comparing the first and second message tag to authenticate the received first contribution.

12. A method of providing secure communications between a first communications unit and a second communications unit, the method comprising a registration step and a key exchange step, wherein the registration step comprises:

generating a first private key value and a corresponding first public key of a key exchange mechanism by the first communications unit;

generating a passcode by the first communications unit;

calculating a message tag of the first public key according to a message authentication code using the passcode by the first communications unit;

making the passcode and the calculated tag value accessible to the second communications unit at least partly by means of a user interaction; and

the key exchange step comprises:

transmitting the first public key by the first communications unit to the second communications unit;

calculating the tag value of the received first public key according to said message authentication code using the passcode by the second communications unit, and accepting the received first public key if the calculated tag value corresponds to the communicated tag value;

generating a second private key value and a corresponding second public key of said key exchange mechanism by the second communications unit;

calculating a shared secret key of said key exchange mechanism from the first public key and the second private key value by the second communications unit;

encrypting the passcode by the second communications unit using the calculated shared secret key;

transmitting the second public key and the encrypted passcode by the second communications unit to the first communications unit;

calculating said shared secret key of said key exchange mechanism from the second public key and the first private key value by the first communications unit; and

decrypting the transmitted encrypted passcode by the first communications unit using the shared secret key calculated by the first communications unit, and accepting the calculated shared secret key if the decrypted passcode corresponds to the passcode originally generated by the first communications unit.

13. A communications system for providing secure communications at least between a first and a second communications unit by means of a key exchange between the first and second communications units resulting in a shared secret key, the key exchange including a user interaction, the communications system comprising :

means for providing, at least partly by means of a user interaction, a passcode to the first and second communications units;

means for generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit;

means for transmitting each generated contribution to the corresponding other communications unit;

means for authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on the passcode; and

means for establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully.

14. A communications system according to claim 13, wherein the first communications unit comprises processing means adapted to generate the passcode and output means for providing the generated passcode to the second communications unit via a second communications channel different from the first communications channel.

15. A communications system according to claim 13, wherein the first and second communications units each comprise processing means for calculating a tag value of a message authentication code, the tag value being calculated from the first contribution and the passcode.

16. A communications system according to claim 15, wherein the processing means are adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode.

17. A communications system according to claim 16, wherein the processing means are further adapted to calculate a hash value of a one-way hash function from the first contribution and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode.

18. A communications system according to claim 16, wherein the error correcting code is a Reed-Solomon code.

19. A communications unit for providing secure communications with another communications unit by means of a key exchange resulting in a shared secret key, the key exchange including a user interaction, the communications unit comprising data processing means, user-interface

means, and a communications interface, the processing means being adapted to perform the following steps:

generating a passcode to be provided at least partly by means of a user interaction via the user-interface means, to the other communications unit;

generating and transmitting via the communications interface a first contribution to the shared secret key, and receiving via the communications interface a second contribution to the shared secret key, the second contribution being generated by the other communications unit;

authenticating the received second contribution based on the passcode; and

establishing said shared secret key from at least the second contribution, only if the received second contribution is authenticated successfully.

20. A communications unit according to claim 19, wherein the processing means is further adapted to calculate a tag value of a message authentication code to be provided to the other communications unit, the tag value being calculated from the first contribution and the passcode.

21. A communications unit according to claim 20, wherein the processing means is further adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode.

22. A communications unit according to claim 21, wherein the processing means is further adapted to calculate a hash value of a one-way hash function from the first contribution and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword

corresponding to the hash value of the first contribution, and the symbol being identified by the passcode.

23. A communications unit according to claim 21, wherein the error correcting code is a Reed-Solomon code.

24. A communications unit according to claim 19, wherein the processing means is further adapted to decrypt an encrypted passcode received together with the second contribution, the decrypting using said shared secret key, and is further adapted to accept the received second contribution only if the decrypted passcode corresponds to the generated passcode.

25. A communications unit for providing secure communications with another communications unit by means of a key exchange resulting in a shared secret key, the key exchange including a user interaction, the communications unit comprising data processing means, storage means, and a communications interface, the processing means being adapted to perform a key exchange resulting in a shared secret key, the key exchange comprising:

receiving, at least partly by means of a user interaction, and storing a passcode generated by another communications unit;

receiving via the communications interface a first contribution to the shared secret key generated by the other communications unit;

authenticating the received first contribution based on the passcode; and

if the received first contribution is authenticated successfully, establishing said shared secret key from at least the first contribution, and transmitting via the communications interface a second contribution to the shared secret key.

26. A communications unit according to claim 25, further adapted to store a message authentication tag in the storage means, and wherein the processing means is adapted to calculate a tag value of a message authentication code from the received first contribution and the passcode, and is adapted to accept the received first contribution only of the calculated tag value corresponds to the stored message authentication tag.

27. A communications unit according to claim 26, wherein the processing means is further adapted to calculate the tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the first contribution, and the symbol being identified by the passcode.

28. A communications unit according to claim 27, wherein the processing means is further adapted to calculate a hash value of a one-way hash function from the first contribution and to calculate said tag value by selecting a symbol of a codeword of an error correcting code, the codeword corresponding to the hash value of the first contribution, and the symbol being identified by the passcode.

29. A communications unit according to claim 27, wherein the error correcting code is a Reed-Solomon code.

30. A communications unit according to claim 25, wherein the processing means is further adapted to encrypt the stored passcode, the encrypting using said shared secret key, and is further adapted to transmit the encrypted passcode with the second contribution via the communications interface to the other communications unit.

31. A computer program product configured to provide secure communications between a first and a second communications unit, comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code for exchanging a key between the first and the second communications units to generate a shared secret key and to receive input from a user;

computer readable program code for providing, at least partly by means of a user interaction, a passcode to the first and second communications units;

computer readable program code for generating a first contribution to the shared secret key by the first communications unit and a second contribution to the shared secret key by the second communications unit, and transmitting each generated contribution to the corresponding other communications unit;

computer readable program code for authenticating the transmitted first and second contributions by the corresponding receiving communications unit based on at least the passcode; and

computer readable program code for establishing said shared secret key by each of the communications units from at least the corresponding received first or second contribution, only if the corresponding received contribution is authenticated successfully.

32. A computer program product configured to provide secure communications with a communications unit, comprising:

a computer readable storage medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code for exchanging a key with the communication unit to generate a shared secret key and to receive input from a user;

computer readable program code for generating a passcode to be provided based on user input to the communication unit;

computer readable program code for generating and transmitting a first contribution to the shared secret key, and receiving a second contribution to the shared secret key, the second contribution being generated by the communication unit;

computer readable program code for authenticating the received second contribution based on the passcode; and

computer readable program code for establishing the shared secret key from at least the second contribution, based on whether the received second contribution is authenticated.